a What is claimed is:

~~Claims~~

1. A secure communication method for allowing a mobile host to communicate with a correspondent host over a Virtual Private Network via a Security Gateway (SG), the method comprising the steps of:

(1) negotiating one or more Security Associations (SAs) between the mobile host and a correspondent host of a Virtual Private Network (VPN);

(2) subsequently initiating a communication between the mobile host and the SG and sending an authentication certificate to the SG, the certificate containing at least the identity of a SA which will be used for subsequent communication between the mobile host and the correspondent host;

(3) sending data packets from the mobile host to the correspondent host using the identified SA, via the SG; and

(4) wherein said data packets are forwarded by the SG to the correspondent host only if they are authenticated by the SG.

2. A method according to claim 1 and comprising, prior to step (2), negotiating one or more Security Associations (SAs) between the mobile host and the SG and sending said authentication certificate to the SG using one of the SAs.

3. A method according to claim 1, wherein said authentication certificate contains an IP address of the mobile host.

4. A method according to claim 1, wherein said SAs are IPsec phase 2 SAs and are used on top of an ISAKMP SA.

5. A method according to claim 4, wherein said authentication certificate contains the ISAKMP cookies of the mobile host 1 and said correspondent host, with which the phase 2 negotiation was done.

6. A method according to claim 1, wherein the SG is coupled between the intranet and a core network of a mobile wireless telecommunications system.

7. A method according to claim 1, wherein the mobile host is a wireless host coupled to the SG via an access network.

8. A method according to claim 1, wherein the VPN comprises an intranet, with the SG being coupled between the intranet and the Internet.

9. A method according to claim 8, wherein said correspondent host resides within the intranet and said data packets are forwarded to the correspondent host from the SG over a secure connection.

10. A method according to claim 1, wherein a negotiated SA expires after a predefined volume of data has been sent using the SA.

11. A method according to claim 1, wherein a negotiated SA is time limited by the SG and, at the end of a predefined time limit, the SA is suspended by the SG.

12. A method according to claim 1, wherein the data packets sent in step (3) and which contain user data are authenticated by the SG using authentication data sent in separate data packets.

13. A method according to claim 2, wherein the data packets sent in step (3) and which contain user data are authenticated by the SG using authentication data sent in separate data packets, and wherein the data packets containing user data are sent using a Security Association (SA) negotiated between the mobile host and said correspondent host and the data packets containing authentication data are sent using a Security Association (SA) negotiated between the mobile host and the SG.

14. A Security Gateway (SG) of a Virtual Private Network, the SG enabling secure communication between a mobile host and a correspondent host, the SG comprising:

(1) means for negotiating one or more Security Associations (SAs) between the mobile host and the Security Gateway (SG);

(2) means for subsequently initiating a communication between the mobile host and the SG using a negotiated SA and for receiving an authentication certificate sent from the mobile host, the certificate containing at least the identity of the mobile host and an IP address of the mobile host;

(3) means for receiving data packets sent from the mobile host and for authenticating the data packets; and

(4) means for forwarding the data packets from the SG to said correspondent host providing that the received data packets are authenticated.

15. A secure communication method for allowing a mobile host to communicate with a correspondent host over a Virtual Private Network, the method comprising the steps of:

(1) negotiating one or more Security Associations (SAs) between the mobile host and a Security Gateway (SG) of a Virtual Private Network (VPN);

(2) subsequently initiating a communication between the mobile host and the SG using a negotiated SA and sending an authentication certificate to the SG, the certificate containing at least the identity of the mobile host and an IP address of the mobile host;

(3) sending data packets from the mobile host to the SG and authenticating the data packets at the SG; and

(4) providing that the received data packets are authenticated, forwarding the data packets from the SG to said correspondent host.

Add A3